A Stochastic Programming Approach to the Design Optimization of Layered Physical Protection Systems

Nathanael Brown, Katherine Jones, Alisa Bandlow,
Lucas Waddell
Sandia National Laboratories
{njbrown, kajones, abandlo, lawadde}@sandia.gov

Linda Nozick
Cornell University
lkn3@cornell.edu

Abstract

The performance of many of the technologies used in physical protection systems that guard high-value assets are heavily influenced by weather and visibility conditions as well as intruder capabilities. This complicates the already difficult problem of optimizing the design of multi-layered physical protection systems. This paper develops an optimization model for the automatic design of these systems with explicit consideration of the impact of weather and visibility conditions as well as intruder capabilities on system performance. An illustrative case study is provided.

1. Introduction

The automatic design of a multi-layered physical protection system (PPS), such as those guarding high-value assets, requires the efficient creation and evaluation of various security architectures without performing an exhaustive enumeration of all possible options. The efficacy of a design should not only consider the delay and detection characteristics, but must also consider the impact that system nuisance/false alarm rates have on the alarm station operators. Additionally, the architecture must be resilient to a variety of environmental conditions and intruder types which impact sensor and barrier performance. The naïve approach of using the average-case representation of the PPS performance characteristics tends to generate an architecture that is highly vulnerable to the worst case scenario and is shown to be inferior to the stochastic optimization approach presented in this paper.

An established approach to evaluating a PPS is to use adversary sequence diagrams (ASDs) to describe the layers of protection that the attacker must pass through in order to reach a target [6]. An ASD typically includes defining detection and delay values for each element along a path to the target. It often represents adjacent areas in diagrams using concentric rectangles. We utilize a layered approach as well, but one that is two-dimensional and focused on the actual physical system layout. For example, impassable obstacles or buildings are represented as voids on the system grid. [3] describes the integration of a human-generated PPS design modeled in 3-D with 2-D design evaluation models. [8] and [11] describe a simulation for design of PPSs integrating Systematic Analysis of Vulnerability to Intrusion (SAVI) [10] for most vulnerable path (MVP) selection. Our approach uses a 2-D projection of a 3-D facility model with automated path identification, architecture generation and evaluation based on allowable design alternatives, intruder capabilities, and environmental factors. As such, our approach reduces PPS design time when compared to [3], [8], [10] and [11] by combining standard MVP design factors to automatically generate architectures, and improves resilience to multiple environmental scenarios. It also creates architectures that trade off performance against investment cost so that decision makers can select the most effective PPS within a fixed budget.

[5] develops an optimization model to select mitigation measures for physical security using historical data on the effectiveness of specific mitigation measures and a multiplicative model to integrate these effects together. In contrast, we employ a game theoretic approach to model the decision-making of the intruder, thereby computing more directly the impacts of security measures. [12] uses Dempster-Shafer evidence theory to develop a risk map of a given architecture and then optimizes that risk map via sensor placement based on a modified averaging approach for belief functions. [7] develops a shortest path algorithm to determine the MVP in a security system. We adopt this

URI: http://hdl.handle.net/10125/41333
ISBN: 978-0-9981331-0-2

computation with some modifications to the implementation described in [4].

2. Model formulation

The model developed in this paper extends the model given in [4] in two significant dimensions. First, scenarios are used to describe the connection between weather, visibility conditions and intruder capabilities with detection probability. Second, the probability of interruption given detection (P_I) is now computed including the impact of nuisance and false alarm rates (NAR/FAR) on operator performance as described in [1]. These modifications yield a more realistic and comprehensive optimization model compared to previous work by treating the alarm station operator (ASO) as an integral part of the PPS and the various environmental scenarios as design considerations.

Suppose there is a network that connects a location with a target. Each link in the network *(i,j)* represents places in which security technology may be located as well as links in the path that the intruder may take. For simplicity we refer to a feasible collection of security technologies for a particular link *(i,j)* as a package. Hence, let I_{ij}^{y} be a binary variable that takes on a value of 1 if investment package *y* is placed on arc *(i,j)* and 0 otherwise. Feasible collections of technologies that can be placed on an arc must be used instead of directly representing the individual technologies, because the combined effects are not generally the same as the sum of the effects of the individual technologies. For example, the probability of detection, (P_D), on an arc when two different technologies are employed is not the sum of the two probabilities. c_{ij}^{y} is the cost of investment package *y* on link *(i,j)* and A_{ij}^{sy} is the NAR/FAR for investment package *y* on link *(i,j)* under scenario *s.* Further, *r* is an index for the paths that connect the intruder origin with the target of interest. Let z^{rs} be a binary variable that takes on a value of 1 if path *r* is taken under scenario *s*. Finally, let g^{rs} be the P_I for path *r* under scenario *s*.

$$\begin{matrix} \max\limits_{I_{ij}^{y}} \left[\min\limits_{z^{rs}} \sum\limits_{r} g^{rs} z^{rs} \right] \\ \min\limits_{I_{ij}^{y}} \left[\sum_{ij} \sum_{y} A_{ij}^{sy} I_{ij}^{y} \right] \\ \min\limits_{I_{ij}^{y}} \left[\sum_{ij} \sum_{y} c_{ij}^{y} I_{ij}^{y} \right] \end{matrix} \qquad (1)$$

Such that

$$\sum_{r} z^{rs} = 1 \ \forall s \qquad (2)$$

$$z^{rs} \in \{0,1\} \ \forall r, s \qquad (3)$$

$$I_{ij}^{y} \in \{0,1\} \ \forall (i,j), y \qquad (4)$$

Equation (1) describes the three objectives of the system owner. The first objective maximizes the P_I the intruder faces. The inner objective expresses the desire of the intruder to minimize their probability of interruption given detection, P_I, by finding the most vulnerable path. Notice that this is done assuming that an architecture is in place and searching over all paths and all scenarios. The outer objective represents the system owner, who is searching over all possible architectures via the decision variables I_{ij}^{y}, to identify the architecture that maximizes the P_I.

It is important to realize that the P_I for a given architecture is scenario-dependent because the P_D for a sensor is dependent on the environmental conditions. Hence for a given architecture, we use the lowest P_I across all environmental conditions (i.e., all scenarios). This is a conservative assumption because it assumes that the intruder has sufficient knowledge to identify the environmental conditions that will maximize their chance of success.

The second objective minimizes the NAR/FAR. The third objective minimizes system costs. These three terms identify a three-dimensional design space from which the optimal architecture is selected. Equation (2) requires that the intruder select a single path under each scenario. Equations (3) and (4) give the binary restrictions on the decision variables.

Many investments are only effective if they are deployed as a cycle or a contiguous boundary instead of possibly disconnected, single-link investments as described in [4]. Consequently, we make use of "layered" investments where a single investment layer consists of a collection of link investments of a single type (e.g., sensor "sX" investments) forming a contiguous boundary around the target at a fixed radius. This strategy decreases the computational complexity by several orders of magnitude while still maintaining high quality solutions.

All link travel times and the Response Force Time (RFT) are treated as Gaussian random variables with a standard deviation of 10% of the mean. Additionally, we treat the ASO processing time (assessment plus queue waiting time), which has a calculated mean value as described in [1], as a Gaussian random variable with a 10% standard deviation. The resultant probability that the RFT (augmented by the ASO processing time) is less than the intruder travel time to the target (after detection) is given by equation (5).

$$P(T_{R+AS} < T_{AT}) = P(T_i) = \varphi\left[\frac{\sum_{j\geq i}\mu_j - (\mu_R + \mu_{AS})}{\sum_{j\geq i}\sigma_j^2 + (\sigma_R^2 + \sigma_{AS}^2)}\right] \quad (5)$$

Where the subscript R is used for the RFT, AS for the ASO processing time, AT for the attacker travel time post detection, i for the index of the link where initial detection occurred, and j for the link index across all indices after detection. The overall P_I based on the P_D on link i, D_i, can then be written as equation (6).

$$P(I) = D_1 P(T_1) + \sum_{i=2}^{n} D_i P(T_i) \prod_{j=1}^{i-1}(1 - D_j) \quad (6)$$

These equations are extensions of the ones defined in [9], which are based on seminal work on P_I in [2], also described in [6]. Since this probability becomes vanishingly small when the initial detection is close to the target, we set a threshold to ignore low probability paths (P_I = 0.1) which mitigates the multipath issue described in [4] when trying to find the MVP (the path with the lowest P_I).

3. Solution procedure

The solution procedure for generating the candidate security architectures uses an investment planning optimization, similar to the one presented in [4]. A genetic algorithm (GA) determines the best mix of investments to apply to the network based on an objective composed of investment cost, NAR/FAR, and P_I. To provide a more realistic RFT, we include an assessment time based on system NAR/FAR using the ASO model described in [1].

Since the investments are now collected in synergistic layers, there is no need to use the region crossover method for genetic crossover as done previously in [4], hence a traditional random cut procedure is used. Each child produced is post-processed to guarantee feasibility by ensuring that at least one layer of each investment type (delay, detection, and ASO) is included, since anything less creates an infeasible solution. If no ASO investments are initially selected, then the minimum number required to keep the NAR/FAR per operator within the "low" range of alarms per day (as defined in [1]) is added. If multiple ASO layers are selected, then the layer with the least number of operators that can feasibly process all alarms is kept, with all others removed.

The initial population is created using a two-stage greedy algorithm, where the first stage creates the minimum required delay strategy, and the second stage adds the detection layers required to give a P_I above a minimum threshold.

The delay stage uses a modified objective that trades off time delay versus investment cost. The minimum path delay must exceed the RFT plus the minimum ASO assessment time with a probability greater than 0.95. The delay investment layers are sorted by incremental benefit (ratio of added delay to investment cost) and applied until the minimum probability is met or exceeded. The detection stage uses a trade-off between investment costs, NAR/FAR, and P_I. The detection layers are initially sorted by decreasing P_D, increasing distance from target, increasing NAR/FAR, and increasing cost (in that order). The sorted collection of investments is applied to the network until P_I is greater than a small threshold (0.1). The minimum number of ASOs required to accommodate the investment NAR/FAR is determined concurrently and is applied as part of the initial investment strategy. At this point, the remaining unused layers (both delay and detection) are sorted by incremental benefit (ratio of increase in P_I to investment cost) and applied until the minimum P_I is met or exceeded. Note that the minimum P_I is generally quite large (on the order of 99%) and the trade-off cost for each detection investment includes the cost of any additional ASOs above those required for the initial investment strategy.

The initial population consists of the greedy investment strategy, as well as a significant number of random strategies (on the order of 1,000). This initial population is used to form the initial efficient frontier, which is then augmented by *cleaning* and *decimating* the efficient frontier and top 5% of solutions closest to the efficient frontier. The *cleaning* process randomly removes as many investment layers as possible without significantly decreasing P_I for each solution examined. The *decimation* process examines each of the cleaned solutions and randomly removes single investment layers, adding each modified solution to the population of solutions (and the efficient frontier, if appropriate) as long as the newly created solution has a P_I above a given threshold (in all experiments in this paper we use 50%).

4. Case study

The illustrative case study is an 11x11 grid with the target in the center. This yields 121 nodes and 420 arcs in the resultant network. Each scenario is based on the intruder's ability to degrade different investments combined with the environmental conditions. We assume that the probability of detection for each sensor, P_D, is impacted differently by the environmental conditions. Table 1 gives the

environmental conditions and their probability of occurrence.

Table 1. Notional environmental scenarios

Environmental Conditions	Abbreviation	Probability of Occurrence
Daytime No Precipitation	DNP	0.5
Daytime With Precipitation	DWP	0.1
Nighttime No Precipitation	NNP	0.3
Nighttime With Precipitation	NWP	0.1

For the purpose of this example, each scenario has two elements: one of the four environmental conditions given in Table 1 and the capability of the intruder. The capabilities of the intruder influence P_D for each sensor (sX, sY, and sZ) as well as the time it takes for the intruder to overcome each fence (F). Table 2 gives notional values (P_D for sensors and delay time in seconds for fences) based on the environmental conditions specified in Table 1.

Table 2. Notional intruder sensor/barrier degrade capabilities under different environmental conditions

	DNP		DWP	
Tech.	**N**	**D**	**N**	**D**
sX	0.80	0.70	0.70	0.60
sY	0.85	0.75	0.82	0.75
sZ	0.60	0.55	0.95	0.8
F	60	30	70	40

	NNP		NWP	
Tech.	**N**	**D**	**N**	**D**
sX	0.4	0.30	0.35	0. 30
sY	0.45	0.30	0.50	0.47
sZ	0.53	0.47	0.85	0.75
F	70	40	80	60

N, D: Normal & Degraded

Table 3 gives the cost, NAR/FAR, and average and worst case detection probabilities for each technology. The last row gives the cost for an ASO.

Table 3: Notional investment cost, NAR/FAR and average/worst case performance

Tech.	10-year Cost ($1000s)	NAR /FAR	Average	Worst Case
sX	$100	3	0.58	0.3
sY	$200	6	0.64	0.3
sZ	$300	12	0.61	0.47
F	$3	0	51.5	30
ASO	$10,000	N/A	N/A	N/A

5. Results

Figure 1 shows the estimated efficient frontier where the three objectives pursued are the worst case P_I (across weather and visibility conditions and attacker types), NAR/FAR (given by the labels) and cost. Only points that had a worst case P_I that exceeds 90% are shown. The architectures range from $120 million to almost $194 million. The $194 million architecture has a worst case P_I = 96.5%.

Figure 2 gives a graph of the average P_I across all scenarios in comparison to the worst case. To create an average value, each intruder type is assumed to be equally likely. This assumption does not impact the optimization because it optimizes across all eight scenarios (four weather and two types of intruders) and focuses on the P_I from the scenario that produces the highest vulnerability. The average difference is on the order of 5%. However, the largest difference is about 7.5%. The average performance for the architecture that costs about $194 million with a worst case P_I = 96.5% has an average P_I = 99.3%.

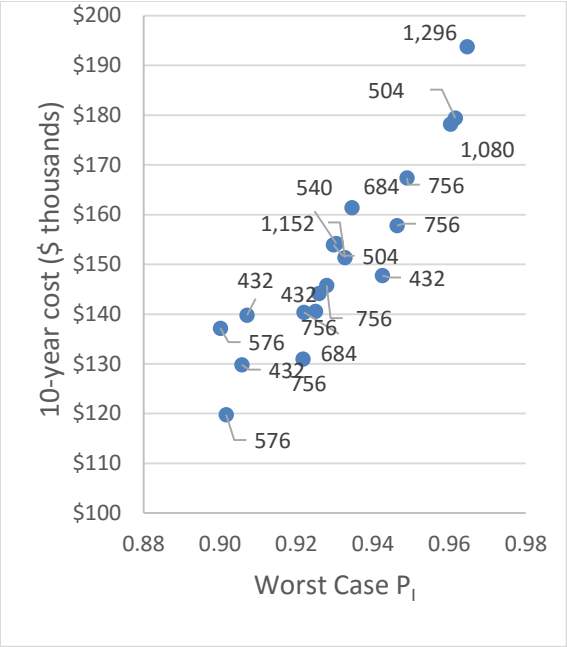

Figure 1. Estimated efficient frontier (solutions with worse case performance that exceeds 90% P_I)

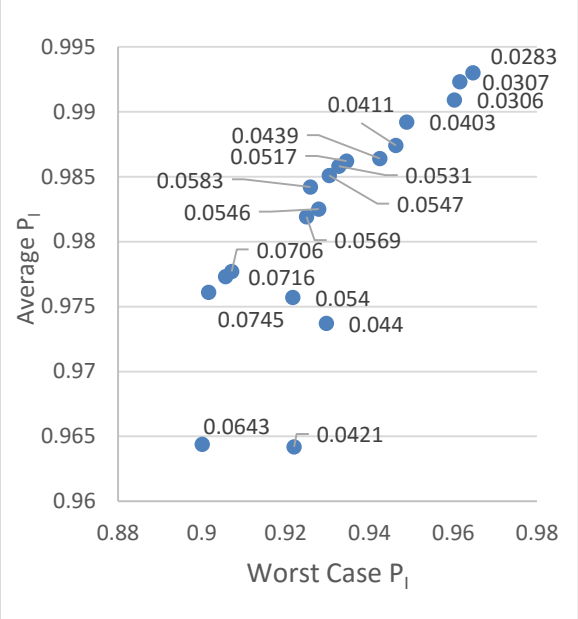

Figure 2. Average P_I vs. worst case for solutions on the frontier given in Figure 1

The best performing (highest P_I on average and worst case) efficient solutions tend to have several key physical characteristics, as illustrated by the PPS architecture in Figure 3. First, fences are built in the investment layers closest to the target, underscoring the desire to slow an intruder down *after* detection, giving the ASOs and response force sufficient time to respond. Second, a diverse collection of sensors is placed towards the outer perimeter of the grid. The diversity ensures that the architecture is effective against all scenarios, as different sensor types are better suited for different environmental conditions. The sensors are most beneficial farther away from the target, since early detection gives the ASOs and response force more time to respond. This sensor placement strategy results in a high NAR/FAR, necessitating the employment of a large number of ASOs. This solution suggests 5 ASOs to combat the almost 1,300 NAR/FAR.

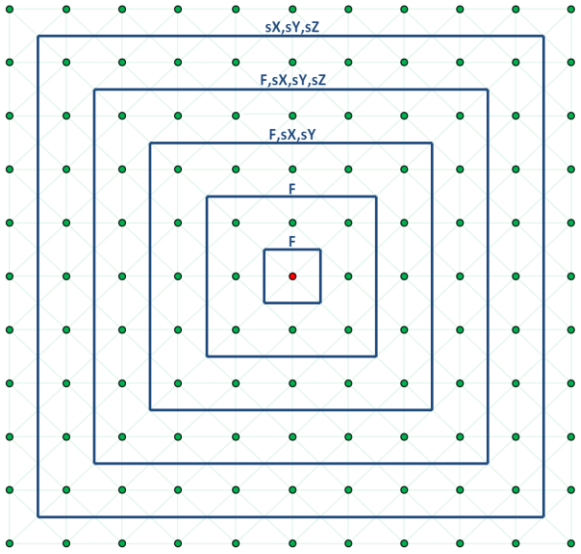

Figure 3. Illustrative solution on efficient frontier (Worst-Case P_I = 0.9647, Average P_I = 0.993, 5 ASO)

High-performing solutions like those in Figure 3 are also extremely costly. In order to reduce the cost of a solution without drastically reducing performance, a typical strategy is to remove sensors from the outermost investment layers, where many sensors are needed per layer. This also reduces NAR/FAR, which means that fewer ASOs are required.

Figure 4 (10-year cost of $119.8M) illustrates a much cheaper but less effective alternative to the solution in Figure 3 (10-year cost of $193.8M), with the expensive but high-performing sY and sZ sensors removed from the outer layer. These two solutions represent the extremes of the efficient frontier pictured in Figure 1.

As an alternative to the stochastic program, a single scenario could be used with average values for the sensor detection probabilities and the fence delay times based on the likelihood of each of the weather conditions and the two types of intruders. A comparison of the value of the solutions identified via this average scenario and those given in Figure 1 provides insight into the value of the stochastic program. To perform this computation, we now use the probability of each scenario explicitly in the optimization.

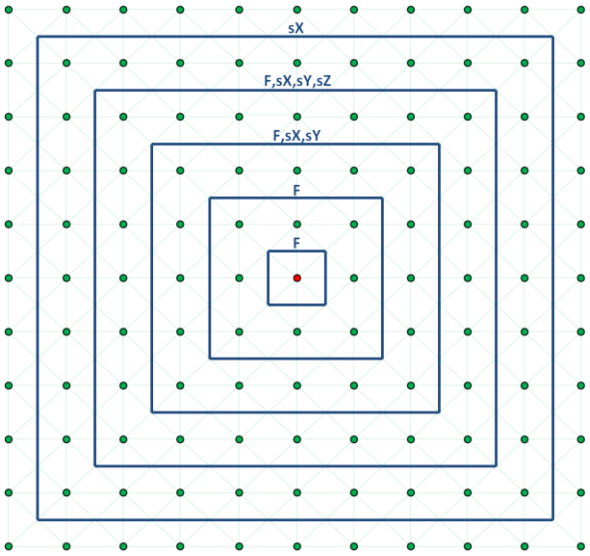

Figure 4. Illustrative solution on efficient frontier (Worst-Case PI = 0.9016, Average PI = 0.9761, 3 ASO)

Figure 5 gives a comparison of the efficient solutions based on an average scenario (circles) and the solutions given in Figure 1 (squares). The diagonal line in Figure 5 indicates solutions for which the worst case P_I is the same as the average (hence there is no variability in the P_I across scenarios). Solutions that are close to this line have less variability in the P_I across scenarios.

The labels are the P_I reported by the optimization for the estimate of the efficient frontier using a single average scenario. Notice that the true mean P_I across all scenarios is generally lower than what the optimization suggests is the P_I (using only the *single* average scenario). The average difference between the true average and what the optimization reports is the P_I is about 9%. Second, there are some solutions for which the optimization reports that the P_I is greater than 90% but the true average across all the scenarios for this architecture is less than 90%. The point labeled with an arrow is just such a situation. The P_I of the average scenario is 93.7%; however, the true average is 79%, and the worst case is 62%. Finally, the worst case is generally substantially worse than the true average. The average difference between the true average and the worst case is about 19%, but that difference reaches about 42% in one of the scenarios.

In contrast, the solutions from Figure 1 (indicated by the squares) have an average performance that is within about 5% of the worst case. The objective does not reward solutions for which the performance is particularly good on some scenarios. Rather, it focuses the trade-off analysis on maximizing P_I for the worst-case scenario (the scenario to which the system is most vulnerable). If we are to assume that the intruder is knowledgeable, this is advantageous.

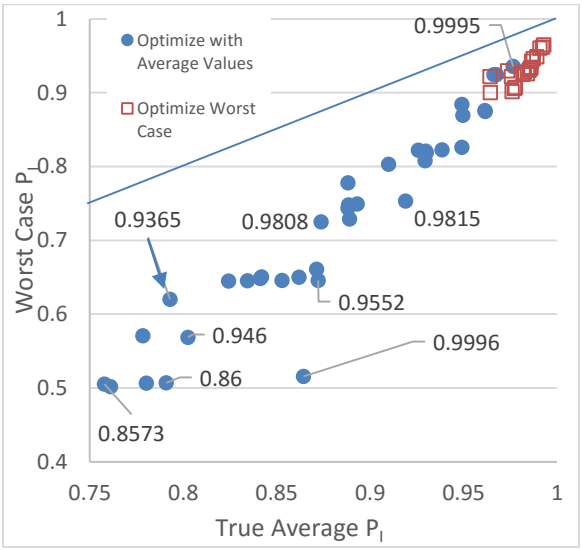

Figure 5. Comparison of the efficient solutions based on an average scenario and the solutions given in Figure 1

6. Conclusion

In order to design a PPS that is resilient to a variety of weather scenarios and intruders with enhanced capabilities, it is critical that a scenario-based optimization approach be employed. As demonstrated by our analysis, trying to create a system that performs well against a spectrum of factors by using an average-case representation of the PPS performance characteristics tends to generate an architecture that is highly vulnerable to the worst case scenario.

Additional research is valuable in at least the following three areas. First, this model assumed a single attacker identifying the weakest path during

the most vulnerable weather and visibility conditions. In practice there may be locations which, if attacked, render other defenses less potent, such as a control center for video surveillance feed, for example. This opens up the possibility that teams of attackers working collectively with different goals may be able to create more potent attacks. Second, this model assumed that the ASOs process alarms in the order received and that there is no priority among the alarms. In practice, some alarms are more reliable than others and some are more important due to their location in the PPS. Integrating priority queuing ideas into the modeling is valuable. Finally, this analysis assumed that each sensor had a fixed NAR/FAR. For many sensors, it is likely that the weather conditions and visibility impact the NAR/FAR. This is easy to incorporate but is also very likely to suggest that ASO staffing could fluctuate based on the environmental conditions.

7. Acknowledgements

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-8382 C

8. References

[1] Bandlow, A., K. Jones, N. Brown and L. Nozick, "The Impact of False and Nuisance Alarms on the Design Optimization of Physical Security Systems", Proceedings of the 7th International Conference on Applied Human Factors and Ergonomics, Advances in Human Factors and System Interactions, 2016.

[2] Bennett, H.A., The "EASI" Approach to Physical Security Evaluation (NUREG-760145), U.S. Nuclear Regulatory Commission, Washington, D.C., 1977.

[3] Bowen, Z., Y. Ming, Y. Hidekazu, and L. Hongxing, "Evaluation of Physical Protection Systems Using an Integrated Platform for Analysis and Design", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016.

[4] Brown, N., K. Jones, L. Nozick, and N. Xu, "Multi-Layered Security Investment Optimization Using Simulation Embedded Within a Genetic Algorithm", Proceedings of the 2015 Winter Simulation Conference, Edited by L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, 2015.

[5] Flammini, F., A. Gaglione, N. Mazzocca, and C. Pragliola, Optimization of Security System Design by Quantitative Risk Assessment and Genetic Algorithms, International Journal of Risk Assessment and Management, 15(2/3), 2011.

[6] Garcia, M., The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Oxford, 2007.

[7] Jang, S., S. Kwak, H. Yoo, J. Kim, and W. Yoon, Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE), Nuclear Engineering and Technology, 41(5), 2009.

[8] Jordan, S., M. Snell, M. Madsen, J. Smith, and B. Peters, Discrete-Event Simulation for the Design and Evaluation of Physical Protection Systems, Proceedings of the 1998 Winter Simulation Conference, 1998, 899-905.

[9] Lemen, E., Adversary Path Determination: Completing, Tuning, and Validating a Genetic Algorithm, Master's Thesis, New Mexico Institute of Mining and Technology, Socorro, NM, 2000.

[10] Matter, J.C., SAVI: A PC-Based Vulnerability Assessment Program, SAND88-1279, July 1988.

[11] Smith, J., B. Peters, S. Jordan, and M. Snell, Distributed Real-Time Simulation for Intruder Detection System Analysis, Proceedings of the 1999 Winter Simulation Conference, 1999, 1168-1173.

[12] Xu, P., Y. Deng, X. Su, X. Chen, and S. Mahadevan, *An Evidential Approach to Physical Protection System Design*, Safety Science, 65, 2014, 125-137.